| IDAHO DEPARTMENT OF PARKS AND RECREATION<br>POLICIES AND PROCEDURES | | | |
|---|---|---|---|
| **Number** | **Effective** | **Title** | **Owner** |
| I-75 | 3/20/06 | Computer Policy | MIS Manager |

Approval: _____

The IDPR has adopted the following policy regarding information systems and technologies; and the acquisition and use of computers, related equipment, and software. This policy recognizes the potential for increasing agency productivity through the appropriate use of information technology, software, and information systems and is intended to promote such use.

## 1.0 PURPOSE:

The purpose of this policy is to establish standards in accordance with state directives for the use and management of computers within the Agency. Specifically, this policy intends to:

- Ensure that the use of computers is consistent with the overall strategy for information management as outlined in the Agency's overall Management Information Systems (MIS)/Information Technology (IT) Plan and is coordinated with other present and planned applications of information technology;
- Establish an appropriate policy structure for the justification, acquisition, and use of computers, related equipment, and software;
- Promote the identification of cost-effective opportunities for using computers to support the mission and program objectives of the Agency;
- Establish accountability for the acquisition and use of computers, related equipment, and software, and;
- Ensure that the integrity and security of automated files, information systems, and program operations are appropriately supported by the use of technology.

## 2.0 SCOPE:

This policy applies to the management and use of all computers, software, applications and electronic devices associated with computers used by the Agency. It applies to all staff utilizing any of these in the performance of their duties for the Agency.

## 3.0 MANAGEMENT AND USER RESPONSIBILITY:

- Responsibility for the use of each computer, as well as for the security of data, equipment, and software associated with that computer, is assigned to the staff person who regularly uses the computer.
- Park and program managers must certify that the acquisition of computers, associated equipment, and computer software is in support of the accomplishment of program or Agency objectives.
- Park and program managers, in conjunction with MIS, are to ensure that adequate computer and software training is provided for all personnel using computer equipment.

## 4.0 INFORMATION TECHNOLOGY COORDINATION:

Coordination of the use and placement of computers and related equipment and software, as well as the technical support for these components, is the responsibility of Management Information Systems (MIS). Included in these responsibilities are the following:

- Assist management and individual employees of the Agency in the identification of opportunities for employing technology and information systems (software and applications) in the improvement of staff productivity;
- Provide technical assistance to computer users;
- Provide configurations for all computers, related hardware, and software acquired for the agency;
- Acquire agency computers, related hardware, and software;
- Provide or coordinate the provision of maintenance and repair services for the Agency's computers and related technology equipment;
- Maintain an ongoing dialogue with agency management to ensure that implemented and proposed applications of Information Technology and Information Systems are consistent with established agency business strategies, missions, goals and objectives;
- Act as technology and information systems liaison for the agency to the Information Technology Resource Management Council (ITRMC), Information Systems Executive Committee (ISEC), and other technology and information systems related focus groups as deemed appropriate;
- Implement the policies, procedures and guidelines established by ITRMC in order to ensure consistency and conformity with statewide information management goals and objectives.

## 5.0 USER RESPONSIBILITY:

- To protect the computer operating systems or operating system components such as the registry and ensure that these components are not modified on computers under their care without the explicit permission and direction of MIS staff.
- To prevent unauthorized persons from accessing agency computer systems and information and to protect the computer systems under their care from unauthorized access.
- To assume sole responsibility for assigned passwords and not disclose personal passwords to anyone.
- To ensure that all files are virus-free before loading or storing any files on an IDPR computer or network.
- To use only software owned by the agency on agency computers unless granted explicit agency approval and in coordination with MIS.
- To adhere to the Information Resource Management Council's (ITRMC) policy on Employee Electronic Mail and Messaging Use found on the Internet at the following URL: http://www2.state.id.us/itrmc/plan&policies/Policies/p1040.htm.
- To adhere to the Information Resource Management Council's (ITRMC) policy on Employee Internet Use found on the Internet at the following URL: http://www2.state.id.us/itrmc/plan&policies/Policies/p1050.htm.
- To adhere to the Information Resource Management Council's (ITRMC) policy on Employee Personal Computer Use found on the Internet at the following URL: http://www2.state.id.us/itrmc/plan&policies/Policies/p1060.htm.
- To maintain agency data with respect to data integrity, data retention, and data backup guidelines as described below.
    - Data Integrity – To ensure that data is input into the system correctly and accurately to the user's best knowledge.
    - Data Retention – To ensure that data is held in accordance with the Agency's policies governing the length of time, format and location.
    - Data Backup - If the user is "file server" connected, to ensure that data is saved to network drives which then are backed up in compliance with practices developed or approved by

MIS for that location. Otherwise, to backup and secure data stored and managed on stand-alone systems or systems not connected to file servers on a schedule that complies with program or Agency policy and practice.

## 6.0 APPROVED EQUIPMENT AND SOFTWARE:

MIS must approve the purchase of information technology hardware and software. MIS will develop the specifications, configure, install, and test all hardware and software.

## 7.0 COMPUTER SOFTWARE DEVELOPMENT:

Commercially developed software, rather than agency developed, will be used whenever possible. The MIS manager and the appropriate program manager and/or project sponsor must approve applications acquired or developed in-house. All application development will be overseen by and/or coordinated through MIS.

## 8.0 CONFIDENTIAL AND SENSITIVE INFORMATION DATA:

All data and information acquired and managed by the IDPR is public information and available upon demand unless specifically protected by statute or rule. The IDPR will secure from unauthorized access all protected data and make a reasonable effort to protect confidential and sensitive information stored in its computer systems.

## 9.0 INFORMATION SYSTEMS ACCESS:

The following section defines access to and disclosure of electronic information, including Email and all other electronic files, maintained on the Agency's computer system. It also sets forth policies on the proper use of the electronic information system provided by the Agency.

9.1 Computer User Setup

When computer access is required for an employee, contract service provider, or volunteer, MIS will create and manage the appropriate access rights and user account structure.

9.2 Security

- Employees may not share system logons and passwords unless authorized by MIS.
- Employees may not use the electronic information systems for purposes of satisfying idle curiosity about the affairs of others with no substantial business purpose for obtaining access to the files or communications of others.
- All electronically stored information is subject to the same requirements of retention and disclosure as hard copy counterparts.
- Access to Electronically Stored Information
    - The creator or proprietor of electronically stored information will manage access to that information in conjunction with MIS.
    - The agency maintains the right to access and disclose the contents of electronically stored files without the consent of the file creator or proprietor.
- Upon separation of an employee, contract service provider, or volunteer, all computer and information systems access will be discontinued for the separated

individual unless otherwise requested by agency or program management, and only if continued access does not pose a threat.

- New computer users assigned to work in data sensitive environments may be assigned limited access rights until such time as the supervisor feels training is complete or experience is sufficient to allow full access.

## 10. SYSTEM BACKUP:

Provision will be made to ensure against the loss of data and programs as a result of machine or power failure, misuse, abuse, or virus attack. Copies of all data files and software will be stored in a safe location. Designate staff at each agency location will perform regularly scheduled backups of data and software. Program management and MIS will monitor this process for compliance. Off-site storage of data backups will be employed whenever possible and where appropriate.

## 11. SOFTWARE INTEGRITY:

The IDPR will strictly adhere to License agreements and copyright protection for software used by the agency. Park and program managers are responsible for enforcing the restrictions, limitations, and agreements associated with proprietary software programs in use at their location.

## 12. MAINTENANCE AND REPAIR:

MIS will provide or make provisions for the repair and routine maintenance of computers and associated equipment. MIS staff or authorized service providers may access system hardware and software “at will” for the purpose of repair and maintenance.

## 13. IT INVENTORY:

IDPR will maintain an inventory of its computer equipment and software.

## 14. POLICY CHANGES:

The IDPR Director will have final approval authority of all MIS policies and policy amendments.